REMARKS

Claims 1-18 are pending in this application. All of the pending claims are rejected. None of the claims are currently amended. Reconsideration is respectfully requested.

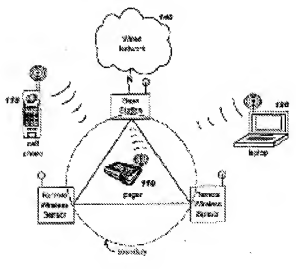
Claims 1-16 are rejected under 35 U.S.C. 103(a) based on US 7,212,828 (Hind) in view of US 6,700,535 (Gilkes). The Office concedes that Hind fails to describe the limitations of transmitting a signal to the client device at less than full power and determining whether the client device responds to the signal, which were added to claims 1 and 14 in the previous response, but asserts that Gilkes describes the limitations at column 28:28-38. Applicant respectfully suggests that Gilkes teaches a variation of the well known technique of calculating position by finding the intersections of circles of uncertainty. In particular, Gilkes describes "location markers" which respond to an inquiry by broadcasting their position in Cartesian coordinates. A mobile device may be aware of its communication range, so it is relatively simple to calculate a circle of uncertainty relative to the responding location markers. For example, if the communication range of the mobile device is 10 meters and location marker "A" responds with position X1, Y1, then the mobile device is somewhere within a circle of 10 meter radius centered on X1, Y1. It is known that in order to more precisely and definitely calculate position with this technique that it is desirable to use multiple circles because the position can be narrowed down to the intersection of those circles of uncertainty. Consequently, it is desirable to transmit the inquiry at a high power level in order to obtain a greater number of responses. Consequently, in the cited passage Gilkes fails to describe reducing transmit power at the mobile device to *determine whether the other device responds*. Rather, Gilke suggests use of different power levels to generate additional circles of uncertainty (with different radii) in order to reduce the area of intersection.

It may be helpful to review the context of the present invention versus the cited references. Gilkes intends to calculate the absolute location of the mobile device in three dimensional space. Note that this requires the use of "location markers" which know their position. Note also that Gilkes only describes how the *mobile device* is able to calculate its own position, which is of no use in a system where the *network* needs to know the position (relative or absolute) of a mobile device that is being authenticated. Hind describes use of location for authentication where the network calculates location of the mobile device. However, Hind requires use of directional antennas and also coordination between devices. Applicant has no reason to believe that the technique described by Hind would not operate satisfactorily. However, the present invention is simpler and less costly to implement. Consider the scenario where a malicious mobile unit broadcasts at an extraordinarily high power (e.g., greater than allowed by the FCC) in order to appear to be close to WLAN devices and thereby be authenticated. Hind determines that the malicious mobile unit is actually far away by triangulating on the malicious mobile unit using directional antennas. As known in the art and illustrated in Hind, at least two separate devices with directional antennas are required to produce an "intersection zone" indicative of the relative or absolute location of the malicious mobile unit. The presently claimed invention is a simpler and arguably more elegant solution. In particular, the authenticating access point does not need to determine the relative or absolute *location* of the malicious mobile unit because the access point simply transmits a reply message to the malicious mobile unit at low power (which the mobile unit does not receive because it is located at a relatively great distance from the access point) in order to *verify range*. Consequently, the claimed invention does not require the "location markers" of Gilkes, or the directional antennas of Hind, or even the cooperation of multiple devices as described by both Gilkes and Hind.

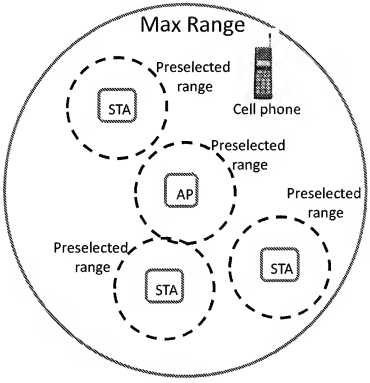
Rather, the authenticating device effectively whispers to the mobile device "if you are so close then tell me if you can hear this."

Claims 17 and 18, which are rejected as being anticipated by Hind under 35 U.S.C. 102(b), are allowable for the reasons already stated in previous responses. As will be explained in greater detail below, and as already emphasized above, *location* is not equivalent to *range*. Hind describes establishment of a spatial boundary defined around a WiFi network. Client devices *located* outside the boundary may be denied access. However, Hind's boundary is not equivalent to the *range* recited in the claims. For example, Hind defines only one boundary for a BSS, the boundary is not centered on a particular device, and the boundary is not limited in any way by the maximum communication range of the network. Rather, Hind's boundary is an *area* defined by remote wireless sensors as shown in figure 3 of Hind, depicted below.

FIG. 3



In contrast with the *boundary* defined by Hind, the preselected *range* recited in the independent claims is defined relative to a network device, and is less than the maximum communication range of the network. Because the *range* is defined by distance to a network device, there can be multiple authentication zones, and those zones are centered on devices. Further, the *range* must be less than the maximum range of the network, which is defined by the location and power of the access point or base station. The following figure illustrates an example of these limitations.



Note that the cell phone is denied authentication because it is not within a preselected range of a network device, even though it is within maximum range of the network, i.e., within range of the AP. An advantage of the recited technique is that network devices tend to be located within a confined work area, and a rogue device located near to one of those devices, i.e., within the work area, is more likely to be a legitimate user than a rogue device located far away from those

devices, i.e., outside the work area. Note that rather than having to define a boundary with specialized sensors as in Hind, the presently claimed invention automatically defines an area based on the locations of devices that are already authenticated. The examiner attempts to equate Hind's boundary with both the preselected range and the maximum communication range, but this is not logical because the recited limitation is that the preselected range is less than the maximum range, not less than or equal. Because Hind fails to anticipate either authentication based on distance to a network device or authentication based on distance relative to maximum communication range, the rejections should be withdrawn.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited. Should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

October 5, 2009
Date

/Holmes W. Anderson/
Holmes W. Anderson, Reg. No. 37,272
Attorney/Agent for Applicant(s)
Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton, MA 01720
(978) 264-4001

Docket No. 160-068
Dd: 10/21/2009